Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method ~~for~~ of communicating to a server machine a certificate of a user which is sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is ~~an HTTP or an equivalent~~ a stateless protocol, and a second ~~security~~ protocol ~~such as SSL or an equivalent protocol is~~ ~~implemented~~ used between the client machine and the security module is a secure stateless protocol, said method comprising:

inserting said certificate into a cookie header of a request in the first protocol;[[,]] and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine;

wherein said certificate has a plurality of separators; and

wherein said cookie header includes a plurality of cookies.

2. (previously presented) A method according to claim 1, further comprising:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header.

3. (currently amended) A method according to claim 1, wherein said inserting step further ~~comprising~~comprises:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine;[[,]] and

creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (currently amended) A method according to claim 3, further comprising:

adding a specific cookie into the existing or new cookie header;[[,]] and

assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

5. (cancelled).

6. (currently amended) A security machine ~~for securing~~which secures exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is ~~an HTTP or an equivalent~~a stateless protocol, and a second ~~security~~ protocol ~~such as SSL or an equivalent protocol is~~ implemented between the client machine and said security machine is a secure stateless protocol, said security machine comprising:

an analyzer ~~for enabling~~which enables the transmission of a certificate inserted into a cookie header of an HTTP or equivalent request;

wherein said cookie header includes a plurality of cookies.

7. (currently amended) A system comprising:

a client machine;[[,]]

a server machine;[[,]] and

a security module;[[,]]

wherein ~~a first protocol used between~~ the client machine and the server machine ~~is an HTTP or an equivalent~~are configured to communicate using a first protocol, said first protocol comprising a stateless protocol;

wherein ~~a second security protocol such as SSL or an equivalent protocol is implemented between~~ the client machine and the security module are configured to communicate using a second protocol, said second protocol comprising a secure stateless protocol;[[,]] and

wherein the security module comprises an analyzing program ~~for enabling~~which enables transmission of a certificate sent by the client machine ~~into~~ in a cookie header of ~~an HTTP or equivalent~~a request in said stateless protocol, wherein said cookie header includes a plurality of cookies.

8. (currently amended) A computer readable medium upon which is embodied a sequence of programmable instructions which, when executed by a security module of a computer system, cause the security module to perform operations comprising:

communicating to a server machine a certificate of a user which is sent by a client machine via the security module, wherein a first protocol used between the client machine and the server machine is a stateless protocol, and wherein a second protocol used between the client machine and the security module is a secure stateless protocol;

inserting said certificate into a cookie header of a request in the first protocol; and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine;

wherein said certificate has a plurality of separators; and

wherein said cookie header includes a plurality of cookies.

~~A program integrated into a security module that allows the method according to claim 1 to be executed when the program is run in a machine.~~